International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3, Issue No.1 pp : 17-21 1 Jan 2014

A Critical Review of Different Cryptographic Technique in Pretty Good Privacy

Sanket Jirapure,Raj Jirapure
Department of Electronics,University of York,York YO10 5DD, UK
sanket.jirapure@gmail.com,raj.jirapures@outlook.com

Abstract— ***E-mail service is one of the most essential Internet Services. E-mail security be composed of confidentiality, authentication and message integrity. Pretty Good Privacy (PGP) is an email security protocol. It helps in encryption of the plain text data giving them cryptographic privacy and authentication. Cryptographic technique is used to encrypt and decrypt data. Cryptography implements to store prime data or transmit it across the receiver so that only recipient can read that data. In this paper, we pointed out the review on different cryptographic techniques for PGP on the basis of difference in working and impact on level of security. We take into consideration the cryptographic technique such as The Rivest-Shamir-Adleman (RSA) and Digital Signature Standard (DSS) for authentication and integrity, the International Data Encryption Algorithm (IDEA) for confidentiality.***

Keywords— ***PGP, RSA, DSS, IDEA, authentication, confidentiality, encryption, CCA, WSN.***

I. INTRODUCTION

Security is one of most prime issue in mail. PGP (Pretty Good Privacy) [1], [2] is extensively used email security standard since 1991 [3]. PGP is a computer program which allows encryption and decryption of plaintext which needs to be protected while communication and also enables users to encrypt electronic mail and a file which needs to be sent from one user to other user. The core idea behind the use of PGP is to ensure strong authentication, confidentiality and integrity by using number of different cryptographic techniques. The main objective of cryptography is the receiver of message should clearly know that the message from the sender is not manipulated in the transfer of the message. Authentication is to make sure that the delivery of the information is from the authorized person to the proposed person for it's used without being tampered in between or altered. Authentication is a method to authenticate or to establish as real who sent the message. Confidentiality is something that a certain thing can only be accessed by its authorized person or to prevent unauthorized reading of the text and integrity means to prevent tampering with the message.

PGP is very secure against the intruder who attack as man in the middle and try to decrypt the information sent as packets in any network. Encryption is used to provide security to a network which is unsecure. The messages encryption is executed using algorithm that are common and known such as International Data Encryption Algorithm (IDEA) [4], Data Encryption Standard (DES) [5], three key Data Encryption Standard (3-DES) [6]. The safety of an encryption algorithm is done using the protection of the key which is called as secret-key encryption where single key is utilized for both encryption and decryption. The key distribution problem is solved by public key algorithm which is called as an asymmetric algorithm that employs a pair of keys. A public key is applied for encryption and a private is applied for decryption. When the data is sent in a session, Hash algorithms provide functions like RSA and DSS is done by PGP for signing up the digital signatures. The signing up of digital signatures is done through the use of private key. An e-mail security is required to render confidentiality, data root authentication, message integrity, non-repudiation of root.

The paper is organized as: In Section II, Background is discussed. In Section III, review on working difference between different cryptographic technique. In Section IV, review on level of security. In Section V, analysis is made. We concluded our work in Section VI.

II. BACKGROUND

For security, Pretty Good Privacy implements authentication by means of the employment of digital signature, confidentiality through the employment of symmetric block encryption and compression by applying the ZIP algorithm. PGP combines mechanism for advancing a public-key reliance model and public-key certificate administration via cryptographic algorithm. A cryptographic algorithm is a numerical function employed in the encryption and decryption technique. It yield in coupling with a key (number, phrase, or word) to cipher the text. The same text encrypts to other encipher text with other keys. The protection of encipher text is fully reliable on the firmness of the cryptographic algorithm design and privacy of the key. PGP is a cryptographic system which consists of cryptographic algorithm, all feasible keys and all the protocols that causes it to perform. PGP provides the option of using number of different techniques in cryptographic for authentication, confidentiality and integrity.

III. WORKING

This part is comprise of working difference of different cryptographic technique in PGP for authentication, confidentiality and integrity. For authentication and integrity, we take into account The Rivest-Shamir-Adleman (RSA) and Digital Signature Standard (DSS) algorithm. For confidentiality, we provided our review on International Data Encryption Algorithm (IDEA).

A. The Rivest-Shamir-Adleman (RSA)

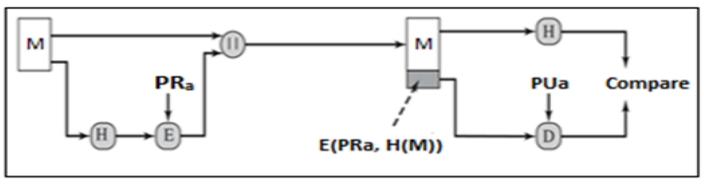

Fig. 1 RSA Approach [7]

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3, Issue No.1 pp : 17-21 1 Jan 2014

RSA [7], [8] is used for public-key cryptography in cryptography technique and also useful for signing, encryption, and decryption. RSA is broadly benefited in e-commerce protocols because of the secure and adequately long keys. The RSA algorithm follows three steps a key generation, encryption, and decryption.

In key generation, it consist of a public key and a private key. For encrypting messages, a public key is used and is known to everyone. A private key [7] is used to decrypt the message which developed at the time of encryption. The keys are generated in four steps. First any two distinct prime numbers p and q is selected. Secondly the modulus for both the public and private keys i.e. n is computed using product of two prime i.e. n = p q. Thirdly, Euler's totient function i.e. φ is Computed using equation φ (n) = (p – 1) (q – 1). Finally, Integer e is selected such that gcd (e, φ (n)) =1, i.e. Public key of RSA is provided by a set of n and e.

In encryption, receiver transmits their public key (n, e) to sender and keeps the private key secret. Sender aspire to transfer message M to receiver where it encrypt the cipher text by using e (m) = m^e (mod n).

In Decryption, receiver regain m from cipher text c by using d(c) = c^d (mod n) which proves the decryption is the inverse of encryption, where d is the multiplicative inverse of e mod φ(n).

The message is signed as an input which produces a fixed length of secured hash code through a hash function in RSA access. The encryption of hash code is done through the private key PRa of the sender in order to create a signature. The message are forwarded further where the acquirer takes the message and yield a hash code. Also the signature put forth further where recipient decipher the signature by applying the sender's public key PUa. The confirmation of authenticate signature is possible only when the hash code meets the deciphered signature as only sender have the authority to certify the signature.

B. Digital Signature Standard (DSS)

After getting the message, the receiver may wish to authenticate that the message has not been changed in travel. Also, the receiver may wish of the identity of sender. DSA support both of these services. A digital signature is an electronic analogue of a written signature to create a digital signature on data and by a validator to authenticate the validity of the signature. Each signatory possess private key and public key which is used in the signature formation process and in the signature authentication process respectively. Secure Hash Algorithm is used to lower the message M in both signature formation and authentication process. Signatures cannot be unauthenticated by one who is unaware of thorough private key of the signatory. But one can validate by using the signatory's public key.

A private and public key pairs is much important from user's point of view. A mandatory bonding of user's public key and user's identity is required to form the bridge between mutually trusted parties.

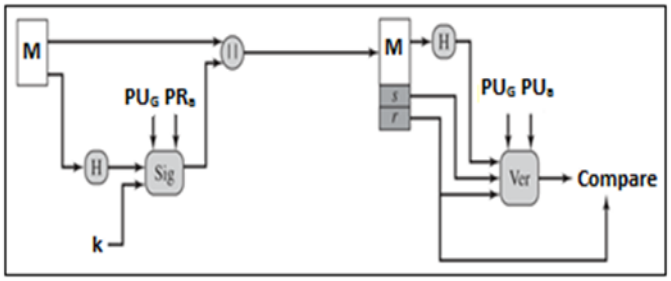

Fig. 2 DSS
Ap

proach [7]

The DSS [7] also makes use of a hash function. A signature function takes the input as a hash code with a random number. A signature function also depends on the sender's private key PR_a and a set constitute to a global public key. The outcome is a signature comprising of two factors, designated as s and r. The verification function takes input of hash code of message plus a signature. The verification function bank on the global public key PU_G and also on the sender's public key PU_a, which is paired with the sender's private key. If a signature is authenticate, the outcome of the verification function is a value. Only the sender with the idea of the private key can yields the valid signature.

C. International Data Encryption Algorithm (IDEA)

IDEA [7] is a block cipher that uses a 128-bit key to encrypt data in blocks of 64 bits plaintext and cipher text. IDEA algorithm comprise of eight rounds followed by a final transformation function as shown in Fig.3.

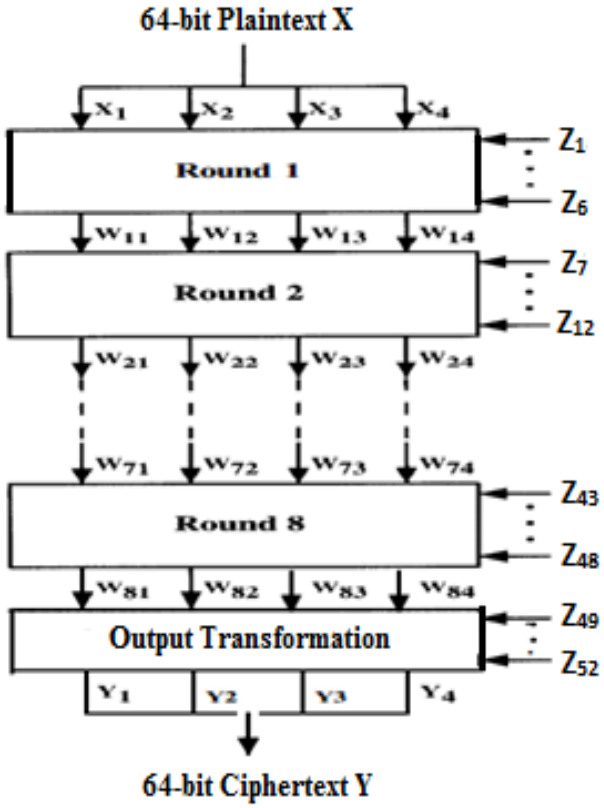

Fig. 3 Overall IDEA Structure [7]

The algorithm structure generally follows three steps such as key generation, encryption and decryption.

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3, Issue No.1 pp : 17-21 1 Jan 2014

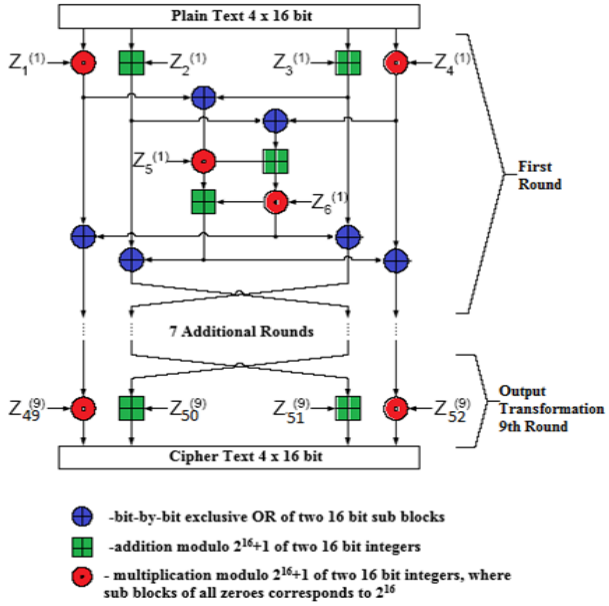

Fig. 4 IDEA Encryption [7]

The operational illustration of encryption process is shown in figure 4. The operation lies of eight encryption step followed by output transformation.

In key generation, the 64 bit plain text block divides the input into four 16-bit sub-blocks. Each of the rounds takes four 16-bit sub-blocks as input and produces four 16-bit output blocks. First, 128-bit key is divided into eight 16-bit sub-blocks, which can be abruptly practiced as eight key sub-blocks. The keys then revolved by 25-bits and disordered again which concluding 128-bit block is again divided into eight 16-bit sub blocks. The shifting above is reproduced until all of the prescribed 52 16-bit blocks have been achieved. The final conversion yields four 16-bit blocks, which are integrated to form the 64-bit cipher text. Subsequent rounds have the same structure but with different sub-key and plaintext-derived inputs.

The four 16 bit key sub-blocks are amalgamate with two 16-bit blocks plaintext blocks using multiplication modulo $2^{16}+1$ and also with the another two plaintext block using addition modulo 2^{16} . It is followed by two 16 bit key sub-blocks with exclusive OR. The final outcome of the first encryption round results in four 16 bit values which are used as input to second encryption round. This operation is repeated for another subsequent 7 encryption round using distant 16 bit key sub-blocks. The encryption round provides final output transformation as the four 16-bit cipher text blocks of the 52 key sub-blocks as shown in Table 1.

Round 1	$Z_1^{(1)}$ $Z_2^{(1)}$ $Z_3^{(1)}$ $Z_4^{(1)}$ $Z_5^{(1)}$ $Z_6^{(1)}$
Round 2	$Z_7^{(2)}$ $Z_8^{(2)}$ $Z_9^{(2)}$ $Z_{10}^{(2)}$ $Z_{11}^{(2)}$ $Z_{12}^{(2)}$
Round 3	$Z_{13}^{(3)}$ $Z_{14}^{(3)}$ $Z_{15}^{(3)}$ $Z_{16}^{(3)}$ $Z_{17}^{(3)}$ $Z_{18}^{(3)}$
Round 4	$Z_{19}^{(4)}$ $Z_{20}^{(4)}$ $Z_{21}^{(4)}$ $Z_{22}^{(4)}$ $Z_{23}^{(4)}$ $Z_{24}^{(4)}$
Round 5	$Z_{25}^{(5)}$ $Z_{26}^{(5)}$ $Z_{27}^{(5)}$ $Z_{28}^{(5)}$ $Z_{29}^{(5)}$ $Z_{30}^{(5)}$
Round 6	$Z_{31}^{(6)}$ $Z_{32}^{(6)}$ $Z_{33}^{(6)}$ $Z_{34}^{(6)}$ $Z_{35}^{(6)}$ $Z_{36}^{(6)}$
Round 7	$Z_{37}^{(7)}$ $Z_{38}^{(7)}$ $Z_{39}^{(7)}$ $Z_{40}^{(7)}$ $Z_{41}^{(7)}$ $Z_{42}^{(7)}$
Round 8	$Z_{43}^{(8)}$ $Z_{44}^{(8)}$ $Z_{45}^{(8)}$ $Z_{46}^{(8)}$ $Z_{47}^{(8)}$ $Z_{48}^{(8)}$
Output Transformation	$Z_{49}^{(9)}$ $Z_{50}^{(9)}$ $Z_{51}^{(9)}$ $Z_{52}^{(9)}$

Table 1. Encryption of Key Sub-blocks

The operational decryption process works same as the encryption but its key material is little hard as it includes the inverse of the sub-blocks. The only contrast with the encryption is that the key blocks must be practiced in the counter order during decryption to reverse the encryption process which is shown in Table 2.

Round 1	$Z_{49}^{(9)-1}$ $-Z_{50}^{(9)}$ $-Z_{51}^{(9)}$ $Z_{52}^{(9)-1}$ $Z_{47}^{(8)}$ $Z_{48}^{(8)}$
Round 2	$Z_{43}^{(8)-1}$ $-Z_{45}^{(8)}$ $-Z_{44}^{(8)}$ $Z_{46}^{(8)-1}$ $Z_{41}^{(7)}$ $Z_{42}^{(7)}$
Round 3	$Z_{37}^{(7)-1}$ $-Z_{39}^{(7)}$ $-Z_{38}^{(7)}$ $Z_{40}^{(7)-1}$ $Z_{35}^{(6)}$ $Z_{36}^{(6)}$
Round 4	$Z_{31}^{(6)-1}$ $-Z_{33}^{(6)}$ $-Z_{32}^{(6)}$ $Z_{34}^{(6)-1}$ $Z_{29}^{(5)}$ $Z_{30}^{(5)}$
Round 5	$Z_{25}^{(5)-1}$ $-Z_{27}^{(5)}$ $-Z_{26}^{(5)}$ $Z_{28}^{(5)-1}$ $Z_{23}^{(4)}$ $Z_{24}^{(4)}$
Round 6	$Z_{19}^{(4)-1}$ $-Z_{20}^{(4)}$ $-Z_{21}^{(4)}$ $Z_{22}^{(4)-1}$ $Z_{17}^{(3)}$ $Z_{18}^{(3)}$
Round 7	$Z_{13}^{(3)-1}$ $-Z_{15}^{(3)}$ $-Z_{14}^{(3)}$ $Z_{16}^{(3)-1}$ $Z_{11}^{(2)}$ $Z_{12}^{(2)}$
Round 8	$Z_7^{(2)-1}$ $-Z_9^{(2)}$ $-Z_8^{(2)}$ $Z_{10}^{(2)-1}$ $Z_5^{(1)}$ $Z_6^{(1)}$
Output Transformation	$Z_1^{(1)-1}$ $-Z_2^{(1)}$ $-Z_3^{(1)}$ $Z_4^{(1)-1}$

Table 2. Decryption of Key Sub-blocks

IV. LEVEL OF SECURITY

Security is one of the most important aspect of any algorithm. Every algorithm is either try to make new changes or try to adapt to current deficit. Depending on the particular algorithm the impact on the level of security is review. So as we have seen the working difference of a particular cryptographic technique like RSA, DSS, and IDEA in PGP, each one has a different technique for a level of security.

RSA incorporates private keys for security. Signature length of RSA is an action of the key length occupied. The system which engage in transitory keys, RSA is not convenient for use in exercise where key generation occurs periodically [9]. There is possible danger to set up a dummy prime which will engage in certain element by undertaking all feasible private keys Using RSA. But it is not possible in presence of private key to approach. B. Schneier [10] describes a method of testing that the numbers used in DSS are ciphered erratically which will result in prime. On the other hand in Chosen Cipher-text Attack (CCA), counter attacker provides an analogues plaintext by electing a number of cipher text through decryption of victim's private key. Thus, the counter attacker picked a plaintext, use the victim's public key to encrypt it, and then decrypt with the private key to reclaim the plaintext. So these are some of the concern related to RSA.

From a protection point of view, one good debate for using DSS keys is the matter that the encryption and signature keys are independent and self-governing now. Independence provides a better security to DSS when attacker try to get the DH private key of someone in comparison with RSA, where revealing a key gives a permission to attacker to see all mails and fabricate a signatures. Also DSS engage in to develop a fixed width signature key regardless of the public or private key size. A signature key produced with DSS is likely to remain safe as it provides an advantage where longer term signature authentication is needed as in Time stamping process [11].

The IDEA algorithm provides a high level of security. Developers has given a first preference to IDEA for data encryption when PGP was invented. IDEA security is

investigate regarding different cryptographic technique analysis which resulted in to state that it is safe to each technique. D. Joan et al. [12] stated that a simple key schedule puts IDEA subject to a class of weak keys that is employing any of a class of 2^{51} weak keys during encryption concluded in simple disclosure and restoration of keys. But available 2^{128} likely keys diminish any strike on security of encryption. Also some keys containing a large number of 0 bits produce weak encryption. When keys is generated randomly, they are of small concern in practice, such that that they are unnecessary to avoid explicitly. A simple fix was proposed: exclusive-OR to each sub-key with a 16-bit constant, such as 0x0DAE [13] which provided full security. Finally with the key of 128 bits in length, IDEA is more secure than widely known encryption scheme.

V. ANALYSIS OF CRYPTOGRAPHIC TECHNIQUE

In this review paper, above defined different cryptographic techniques are investigated based on various research paper in respective journal.

R. Schlafly [14] concluded that both (RSA and DSS) of these algorithms are built around probably incompliant issues that have been gone through the investigation by the cryptographers from all around the world. The approach of RSA and DH based systems are identical but in practice RSA keys turns up more susceptible. RSA is an algorithm for public-key cryptography that is based on the difficulty of factoring large integers, the factoring problem. A user of RSA publishes the product of two large prime numbers with their public key. The prime factors must be kept secret. Anyone can encrypt a message by using public key. But with recent methods, there is possibility of decrypting the message by someone who has an idea of the prime factors if the public key is large enough. Wireless Sensor Network (WSN) is susceptible and unsecure to many attacks because wireless medium is broadcast in nature. Hence RSA is not relevant for Wireless Sensor Network because of high time intricacy and utilization demand [15]. There is not any literature that foresees that either RSA or DH are more or less safe than the other given correct implementation cryptograph in operation. Digital signature algorithm is used by receiver end to authenticate that the message has not been modified during travel as well as to identify the sender. To provide security to stored data, Digital signatures can be created so that integrity of the data may be authenticated latter. One method suggested by Erfaneh Noorouzil [16] makes use of Hash function to produce fickle or smaller size of bits which rely on each bytes of data for transmitting low size and volume data by using DSA.

IDEA is believe to be secure on the basis of universal consideration of both the cipher progress and its theoretical basis. It permits the effective security of transmitted and stored data against unauthorized access by third parties. IDEA's security implements action on three other algebraic class. Investigation of different fault attacks regarding block cipher on IDEA suggested that it employs a multiplication modulo to create disorder instead of containing substitution tables. Collision Fault Analysis (CFA) [17] does not allow to reveal a sufficient amount of key material to pose a real threat, which is based on a restrictive fault model. On the other hand, Ineffective Fault Analysis (IFA) [18], [19] compatible to same fault model, gives authorization to get back the entire key in the sacrifice of a maximum quantity of fault injections. In this light, a Differential Fault Analysis (DFA) [20] which seems to be of particular interest to an attacker, grants a permission to improve a significant and strong part of the key by allowing a minimum quantity of fault injections in the most regular fault model.

VI. CONCLUSION

This paper presents a review on number of different cryptography technique for authentication, integrity and confidentiality in Pretty Good Privacy (PGP). It take into account various cryptographic technique algorithm mainly focusing on working difference with security measurement. After reviewing all the above techniques, it can be concluded that a digital signature is employed by receiver in DSA to certify that the signal obtained is unchanged. RSA is public key cryptography that is based on the assumed adversity of factoring large integers. IDEA is a strong block cipher by mixing operations from different algebraic group. IDEA is a patented and universally applicable block encryption algorithm with a key of 128 bits in length which makes it more secure.

REFERENCES

i. *J. Callas, "Open PGP Specification and Sample Code", Printers Inc. Bookstore, Palo Alto, March 1999.*

ii. *S. Garnkel, "PGP: Pretty Good Privacy", O'Reilly & Associates, 1995.*

iii. *P. Zimmermann, "The Official PGP User's Guide", MIT Press, 1995.*

iv. *X. Lai, J. L. Massey and S. Murphy, "Markov Ciphers and Differential Cryptanalysis", Advances in Cryptology EUROCRYPT '91, Lecture Notes in Computer Science, Springer-Verlag, pp. 17-38, 1991.*

v. *FIPS PUB 46-3, "Data Encryption Standard", Federal Information Processing Standards (FIPS), Publications (46-3), National Institute of Standards and Technology, US Department of Commerce, Washington D.C., October 1999.*

vi. *ANSI X9.52. "Triple Data Encryption Algorithm Modes Of Operation", American National Standards Institute, July 29, 1998.*

vii. *W. Stalling, "Cryptography and Network Security Principles and Practice". London: Prentice Hall, 2011.*

viii. *M. Rani, A. Rose, and M. Chawla," Review Of Public Key Cryptography On wimax Using RSA Algorithm", Vol. II, pp. 219-222, October-December, 2011. [Online]. Available: www.technicaljournalsonline.com/jers/VOL%20II/JERS, [Accessed: 1 Oct 2013]*

ix. *B. Schneier, and C. Hall, "An Improved E-Mail Security Protocol", Thirteen Annual Computer Security Applications Conference, ACM Press, Dec 1997, pp. 232-238.*

x. *B. Schneier, "Applied Cryptography Second Edition", John Wiley & Sons, 1996.*

xi. *A. Odlyzko, "The Future of Integer Factorization", RSA CryptoBytes, Volume 1, 2nd November 1995.*

xii. *D. Joan, G. Rene, and V. Joos, "Weak Keys for IDEA", Advances in Cryptology, CRYPTO 93 Proceedings, pp. 224-231, 1993.*

xiii. *J. Nakahara, B. Preneel, and J. Vandewalle, "A Note on Weak Keys of PES, IDEA and some Extended Variants", 7th Oct 2002.*

xiv. *R. Schlafly, "Re: Opinions on S/MIME" sci. crypt USENET Posting, 30th December 1998.*

xv. *F. Amin, A. H. Jahangir and H. Rasifard, "Analysis of Public key Cryptography for Wireless Sensor Networks Security," In Proceedings of World Academy of Science, Engineering and Technology, ISSN 1307-6884, 2008.*

xvi. *E. Noorouzil, "A New Digital Signature Algorithm", International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011.*

xvii. L. Hemme, "A Differential Fault Attack Against Early Rounds of (Triple-) DES", Cryptographic Hardware And Embedded Systems 04, Volume 3156 of Lecture Notes in Computer Science, pp. 254-267, 2004.

xviii. J. Blomer, and J. Seifert, "Fault Based Cryptanalysis of the Advanced Encryption Standard", Financial Cryptography 03, Volume 2742 of Lecture Notes in Computer Science, pp. 162–181, 2003.

xix. C. Clavier, "Secret External Encodings Do not Prevent Transient Fault Analysis", Cryptographic Hardware and Embedded Systems-CHES '07, volume 4727 of Lecture Notes in Computer Science, pp. 181–194, 2007.

xx. E. Biham, and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems", Advances in Cryptology–CRYPTO'97, Volume 1294 of Lecture Notes in Computer Science, pp. 513–525, 1997.